



TITLE:

# Azumaya Algebras and Skew Polynomial Rings (Skew Polynomial Rings, Group Rings and Related Topics)

AUTHOR(S):

IKEHATA, SHUICHI

---

CITATION:

IKEHATA, SHUICHI. Azumaya Algebras and Skew Polynomial Rings (Skew Polynomial Rings, Group Rings and Related Topics). 数理解析研究所講究録 1981, 438: 23-28

ISSUE DATE:

1981-09

URL:

<http://hdl.handle.net/2433/102785>

RIGHT:

# AZUMAYA ALGEBRAS AND SKEW POLYNOMIAL RINGS

Shuichi IKEHATA

Department of Mathematics, Okayama University

This note is an abstract of the author's paper [1] and includes some improvements of the results in it.

Throughout this note, every ring has identity 1, its subring contains 1, and every module over a ring is unital. A ring homomorphism means such one sending 1 to 1. In what follows,  $B$  will represent a ring,  $\rho$  an automorphism of  $B$ ,  $D$  a  $\rho$ -derivation of  $B$  (i.e. an additive endomorphism of  $B$  such that  $D(ab) = D(a)\rho(b) + aD(b)$  for all  $a, b \in B$ ). Let  $R = B[X; \rho, D]$  be the skew polynomial ring in which the multiplication is given by  $aX = X\rho(a) + D(a)$  ( $a \in B$ ). By  $R_{(0)}$ , we denote the set of all monic polynomials in  $R$  with  $gR = Rg$ .

A ring extension  $B/A$  is called to be separable if the  $B$ - $B$ -homomorphism of  $B \otimes_A B$  onto  $B$  defined by  $a \otimes b \rightarrow ab$  splits, and  $B/A$  is called to be H-separable if  $B \otimes_A B$  is  $B$ - $B$ -isomorphic to a direct summand of a finite direct sum of copies of  $B$ . As

is well known, an H-separable extension is separable. A polynomial  $g$  in  $R_{(0)}$  is called to be separable (resp. H-separable) if  $R/gR$  is a separable (resp. H-separable) extension of  $B$ . Moreover, a ring extension  $B/A$  is called to be G-Galois if there exists a finite group  $G$  of automorphisms of  $B$  such that  $A = B^G$  (the fixed ring of  $G$  in  $B$ ) and  $\sum_i x_i \sigma(y_i) = \delta_{1,\sigma}$  ( $\sigma \in G$ ) for some finite  $x_i, y_i \in B$ .

We shall use the following conventions:

$U(B)$  = the set of all invertible elements in  $B$ .

$u_l$  (resp.  $u_r$ ) = the left (resp. right) multiplication effected by  $u \in B$ ,  $B_l = \{u_l \mid u \in B\}$ .

$B^0 = \{a \in B \mid \rho(a) = a\}$ ,  $B^D = \{a \in B \mid D(a) = 0\}$ .

1. H-separable polynomials. In our study, H-separable polynomials in skew polynomial rings play important rôles. Therefore, this section is devoted to giving some results concerning H-separable polynomials. Throughout, let  $f = X^m + X^{m-1}a_{m-1} + \dots + Xa_1 + a_0$  be in  $B[X; \rho, D]$  and  $m \geq 2$ . First, we state the following which is easily obtained from the result of Miyashita [2, Theorem 1.9].

Theorem 1.1. Let  $f$  be in  $R_{(0)}$ , and  $I = fR$ . If  $f$  is an H-separable polynomial in  $R$ , then there exist  $y_i, z_i \in R$  with  $\deg y_i < m$  and  $\deg z_i < m$  such that  $ay_i = y_i a$ ,  $\rho^{m-1}(a)z_i = z_i a$  ( $a \in B$ ) and

$\sum_i y_i x^{m-1} z_i \equiv 1 \pmod{I}$ ,  $\sum_i y_i x^k z_i \equiv 0 \pmod{I}$  ( $0 \leq k \leq m-2$ ), and conversely.

By virtue of Theorem 1.1, we have the following

**Proposition 1.2.** Let  $f$  be in  $R_{(0)} = B[X; \rho]_{(0)}$ . If  $f$  is  $H$ -separable in  $R$ , then  $a_0 \in U(B)$ ,  $\rho(a_0) = a_0$ ,  $\rho^m = (a_0^{-1})_L (a_0)_R$ , and  $f = X^m + a_0$ . Moreover,  $\{g \in R \mid g \text{ is } H\text{-separable}\} = \{X^m + b_0 \mid b_0 \in U(Z \cap B^0) a_0\}$ , where  $Z$  is the center of  $B$ .

**Proposition 1.3.** Let  $f$  be in  $R_{(0)} = B[X; D]_{(0)}$ . If  $f$  is  $H$ -separable in  $R$ , then  $B$  is of prime characteristic  $p$ , and  $f$  is a  $p$ -polynomial of the form  $\sum_{j=0}^e x^{p^j} b_{j+1} + b_0$  ( $p^e = m$ ). Moreover,  $\{g \in R \mid g \text{ is } H\text{-separable}\} = \{\sum_{j=0}^e x^{p^j} b_{j+1} + \beta \mid \beta - b_0 \in Z \cap B^D\}$ .

2. Azumaya algebras induced by  $B[X; \rho]$ . Throughout this section,  $B$  will mean a commutative ring,  $\rho$  an automorphism of  $B$ ,  $G$  the cyclic group generated by  $\rho$ ,  $A = B^G = B$ , and  $R = B[X; \rho]$ .

**Theorem 2.1.** Let  $f = X^m + X^{m-1} a_{m-1} + \dots + X a_1 + a_0$  be in  $R_{(0)}$ , and  $S = R/fR$ . Then,  $f$  is  $H$ -separable in  $R$  if and only if  $S$  is an Azumaya  $A$ -algebra. When this is the case, there holds that  $B/A$  is  $G$ -Galois, the order of  $G$  is  $m$ ,  $f = X^m + a_0$ , and  $a_0 \in U(A)$ .

Theorem 2.2. The following conditions are equivalent:

- (a)  $B/A$  is a  $G$ -Galois extension with  $G$  of order  $m$ .
- (b)  $R_{(0)}$  contains an  $H$ -separable polynomial of degree  $m$ .
- (c)  $R_{(0)}$  contains a polynomial  $f$  of degree  $m$  such that  $R/fR$  is an Azumaya  $A$ -algebra.
- (d)  $\{g \in R \mid g \text{ is } H\text{-separable}\} = \{X^m + a \mid a \in U(A)\}$ .

When this is the case, for every  $a \in U(A)$ ,  $B$  is a maximal commutative  $A$ -subalgebra of  $R/(X^m + a)R$ ,  $(R/(X^m + a)R) \otimes_A B \cong B \otimes_A (R/(X^m + a)R) \cong M_m(B)$ , and moreover, if  $m \in U(A)$  then  $A[X]/(X^m + a)A[X]$  is a separable splitting ring for  $R/(X^m + a)R$ .

Theorem 2.3. Assume that  $R$  contains an  $H$ -separable polynomial of degree  $m \geq 2$ . For  $f \in R_{(0)}$ , the following conditions are equivalent:

- (a)  $f$  is separable in  $R$ .
- (b)  $f = g(X^m)$  or  $Xg(X^m)$  for some  $g(t)$  in  $A[t]_{(0)}$  such that  $g(t)$  is separable in  $A[t]$  and the constant term of  $g(t)$  is in  $U(A)$ .
- (c)  $R/fR$  is a separable  $A$ -algebra.

3. Azumaya algebras induced by  $B[X;D]$ . Throughout this section,  $B$  will mean a commutative ring,  $D$  a derivation of  $B$ ,  $A = B^D$  and  $R = B[X;D]$ .

Theorem 3.1. Let  $f \in R_{(0)}$ ,  $\deg f = m$ , and  $S = R/fR$ . Then the following conditions are equivalent:

- (a)  $f$  is  $H$ -separable in  $R$ .
- (b)  $S$  is an Azumaya  $A$ -algebra.
- (c) There exist  $y_i, z_i \in B$  such that  $\sum_i D^{m-1}(y_i)z_i = 1$  and  $\sum_i D^k(y_i)z_i = 0$  ( $0 \leq k \leq m-2$ ).

Theorem 3.2. The followings are equivalent:

- (a)  ${}_A B$  is a finitely generated projective module of rank  $m$  and  $\text{Hom}({}_A B, {}_A B) = B[D]$  (the subring generated by  $B_\ell$  and  $D$ ).
- (b)  $R$  contains an  $H$ -separable polynomial  $f$  of degree  $m$ .
- (c)  $R_{(0)}$  contains a polynomial  $f$  of degree  $m$  such that  $R/fR$  is an Azumaya  $A$ -algebra.
- (d)  $R_{(0)}$  contains a polynomial  $f$  of degree  $m$ , and there exist  $y_i, z_i \in B$  such that  $\sum_i D^{m-1}(y_i)z_i = 1$  and  $\sum_i D^k(y_i)z_i = 0$  ( $0 \leq k \leq m-2$ ).

When this is the case, for any  $H$ -separable polynomial  $f$ , there holds the following:

- (1)  $R = B[X;D]$  is an Azumaya  $A[f]$ -algebra such that  $B[f]$  is a maximal commutative  $A[f]$ -sub-

algebra of  $R$  with  $B[f] \otimes_{A[f]} R \cong R \otimes_{A[f]} B[f] \cong M_m(B[f])$ .

(2)  $B$  is a maximal commutative  $A$ -subalgebra of  $R/fR$  with  $B \otimes_A (R/fR) \cong (R/fR) \otimes_A B \cong M_m(B)$ .

Theorem 3.3. Assume that  $R$  contains an  $H$ -separable polynomial  $f$ . Let  $\Psi : A[t] \rightarrow R$  be defined by  $\Psi(g_0(t)) = g_0(f)$ .

(a)  $\Psi$  induces a one-to-one correspondence between  $A[t]_{(0)}$  and  $R_{(0)}$ .

(b) For  $g_0 \in A[t]_{(0)}$ ,  $g_0$  is separable in  $A[t]$  if and only if  $R/\Psi(g_0)R$  is a separable  $A$ -algebra, and moreover,  $\Psi(g_0)$  is  $H$ -separable in  $R$  if and only if  $\deg g_0 = 1$ .

#### References

- [1] S. Ikehata: Azumaya algebras and skew polynomial rings, Math. J. Okayama Univ., 23(1981), 19 - 32.
- [2] Y. Miyashita: On a skew polynomial ring, J. Math. Soc. Japan 31(1979), 317 - 330.